UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

MICHAEL VARLOTTA, individually and on behalf of all others similarly situated, Plaintiff, v. NELNET SERVICING, LLC, Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Michael Varlotta ("Plaintiff") brings this Class Action Complaint against NELNET SERVICING, LLC ("Defendant" or "Nelnet"), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant Nelnet Servicing, LLC a Lincoln, Nebraska based student loan servicing company to seek damages for himself and other similarly situated current and former student loan borrowers ("borrowers"), or any other person(s) impacted in the data breach at issue ("Class Members") who he seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members. This action arises from Defendant's failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted and unredacted names, email addresses, phone numbers, and Social Security numbers (collectively, "personal identifiable information" or "PII").

2. Plaintiff alleges Nelnet failed to provide timely, accurate and adequate notice to Plaintiff and Class Members who were or are student loan borrowers whose PII was handled by Nelnet's for the purpose of processing student loan payments. Current and former borrowers' knowledge about what PII Nelnet lost, as well as precisely what types of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Nelnet's unreasonable notification delay after it first learned of the data breach.

3. On or about August 26, 2022, Nelnet notified state Attorney Generals about a widespread data breach involving sensitive PII of 2,501,324 individuals.[1] Nelnet explained in the required notice letter that it discovered an unauthorized third-party gained access to a portion of Nelnet's system. Nelnet discovered that files on its network were accessed and acquired by the unauthorized actor (the "Data Breach").

4. On July 21, 2022, Nelnet chose not to notify affected borrowers or, upon information and belief, anyone of its data breach instead choosing to address the incident in-house by implementing other alleged safeguards to some aspects of its computer security.

5. Approximately a month later, on August 17, 2022, Nelnet concluded its investigation and notified Plaintiff and Class Members that their PII had been impacted and was accessed on its network.[2]

6. Nelnet conducted an investigation to determine whether personal information hosted on its network may have been impacted as a result of the incident, and determined that Plaintiff's and Class Members' PII (including but not limited to full name and Social Security

[1] Office of the Maine Attorney General, *Data Breach Notifications*, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml (last accessed August 29, 2022).
[2] *Id.*

number) was impacted and stolen by the unauthorized person during the Data Breach.[3]

7. Plaintiff and the Class Members in this action were, upon information and belief, current and former student loan borrowers with their PII on Nelnet's system. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters on August 26, 2022.

8. In its Notice Letters, sent to Plaintiff and Class Members, Nelnet failed to explain why it took the company over a month (from July 21, 2022, when Nelnet detected unusual activity to August 26, 2022) to alert Class Members that their sensitive PII had been exposed. As a result of this delayed response, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm.

9. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Nelnet's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' sensitive data. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Nelnet's failure to: (i) adequately protect Plaintiff and Class Member PII; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) effectively monitor Nelnet's network for security vulnerabilities and incidents. Nelnet's conduct amounts to negligence and violates federal and state statutes. Plaintiff and Class Members have suffered injury as a result of Nelnet's conduct.

---

[3] *Id.*

These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (v) charges and fees associated with fraudulent charges on their accounts, and (vi) the continued and certainly an increased risk to their PII, which remains in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

11. Nelnet disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As the result, Plaintiff's and Class Members' PII was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

12. Plaintiff Michael Varlotta is a resident and citizen of Illinois. He received Nelnet's *Notice of Security Incident*, dated August 26, 2022, by U.S. Mail.

13. Defendant Nelnet Servicing, LLC is a Lincoln, Nebraska based student loan servicing company, which has a principal place of business at 121 S. 13TH Street, Suite 100, Lincoln, Nebraska 68508.

14. Defendant Nelnet Servicing, LLC is a wholly-owned subsidiary of Nelnet Diversified Solutions LLC, a Lincoln, Nebraska based limited liability company, which is itself a wholly-owned subsidiary of Nelnet Inc., a Lincoln, Nebraska based corporate conglomerate that deals in the administration and repayment of student loans and education financial services.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Nelnet and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to

establish minimal diversity.

18. The District of Nebraska has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Nebraska and this District through its headquarters, offices, parents, and affiliates.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

20. Defendant Nelnet Servicing, LLC is a Lincoln, Nebraska based student loan servicing company, which has a principal place of business at 121 S. 13TH Street, Suite 100, Lincoln, Nebraska 68508.

21. In its Notice of Data Breach letter to victims of the Data Breach, Nelnet claims that it takes the privacy and security of your information very seriously, stating, "The confidentiality, privacy, and security of our customers' information is one of our highest priorities." [4]

22. Plaintiff and the Class Members, as current or former student loan borrowers, reasonably relied (directly or indirectly) on this sophisticated student loan servicing company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Borrowers, in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

[4] *Id.*

23. Nelnet had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

24. Defendant's Privacy Policy ("Privacy Policy") states, "Protecting your privacy is important to Nelnet and our employees ... We implement reasonable and appropriate physical, procedural, and electronic safeguards to protect your information."[5]

25. Defendant's Privacy Policy applies to any personal information provided to Nelnet and any personal information that Nelnet collects from its website, affiliates, and mobile apps.[6]

26. Defendant's Privacy Policy does not permit Defendant to use and disclose Plaintiff's and Class Members' Private Information unless complying with laws or to carry out internal functions.[7]

27. The Privacy Policy further states,

> Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection.[8]

28. Defendant violated its own Privacy Policy by unlawfully disclosing Plaintiff's and Class Members' Private Information to third parties.

[5] https://www.nelnet.com/privacy-and-security
[6] *Id.*
[7] *Id.*
[8] *Id.*

The Data Breach

29. On August 26, 2022, Nelnet first began notifying state Attorneys General ("AGs") and Class Members about a widespread data breach of its computer network involving the sensitive personally identifiable information of consumers.[9]

30. According to its Notice Letters to Class Members, Nelnet explained it discovered on July 21, 2022 (over a full month earlier) that it detected an unauthorized third-party gained access to a portion of its information system and network.[10]

31. On or about August 26, 2022, Nelnet notified state Attorneys General about a widespread data breach involving sensitive PII of 2,501,324 individuals.[11]

32. In July 2022, Nelnet chose not to notify affected Class Members, or upon information and belief, anyone, of its data breach instead choosing to address the incident in-house by implementing other safeguards to some aspects of its computer security. It then simply resumed its normal business operations.

33. Over a month later, on August 26, 2022, Nelnet admitted that Class Members' PII had been impacted and taken from its network.

34. The notice letters Nelnet instructed to be sent to Plaintiff and Class Members noted that the unauthorized actors had access to Nelnet's system from June 2021 through July 21, 2022, which is a very long time for an unauthorized actor to be permitted access to Plaintiff's and Class Members' PII while inside of Nelnet's system without detection.

35. Nelnet "launched an investigation with third-party forensic experts" of Nelnet's

[9] https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml; https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-521.pdf.
[10] *Id.*
[11] *Id.*

systems, and determined that Plaintiff's and Class Members' personally identifiable information (including but not limited to full names and Social Security numbers) was present and likely stolen by the unauthorized person at the time of the incident.[12]

36. The letters Nelnet directed to be sent to borrowers, including Plaintiff and Class Members, noted unequivocally that their PII was impacted by the Data Breach.

37. Plaintiff and Class Members in this action were, upon information and belief, current and former student loan borrowers whose PII was utilized by Nelnet for purposes of servicing student loan payments. Plaintiff and Class Members first learned of the Data Breach when they received by U.S. Mail Notice of Data Breach letters dated August 26, 2022.

38. Upon information and belief, the PII was not encrypted prior to the Data Breach.

39. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

40. Beginning on or about August 26, 2022, Nelnet sent affected persons (including Plaintiff) a written correspondence regarding the Data Breach, informing the recipients that their confidential data was involved.

41. Nelnet admitted in its written correspondence to the affected persons that their systems were subjected to unauthorized access from June 1, 2022, until July 22, 2022.[13] Nelnet made no indication to either state Attorneys General or the Class Members that the exfiltrated PII was retrieved from the cybercriminals who took it.

42. In response to the Data Breach, Nelnet claims it has further secured their systems to protect the private information. Nelnet admits additional security was required, but there is no

[12] *Id.*
[13] *Id.*

indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

43. Nelnet had obligations created by contract, industry standards, common law, and representations made to student loan borrowers to keep Plaintiff's and Class Members' PII confidential, and to protect the PII from unauthorized access and disclosure.

44. Plaintiff and Class Members provided their PII to Nelnet and/or its affiliates with the reasonable expectation that Nelnet as a sophisticated company would comply with its duty and obligations and representations to keep such information confidential and secure from unauthorized access.

45. Nelnet failed to uphold its data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

46. Nelnet did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

47. Nelnet could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

48. In notice letters, regarding the Data Breach, Nelnet acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of Nelnet's business purposes. Nelnet acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take

reasonable steps to protect PII from improper release or disclosure.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

49. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

50. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[14]

51. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[15]

52. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[16]

53. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

54. Individuals are particularly concerned with protecting the privacy of their financial account information, which are the "secret sauce" that is "as good as your DNA to hackers."

55. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June

---

[14] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed December 10, 2021)
[15] *Id.*
[16] *Id.* at p. 15.

2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Nelnet knew or should have known that its electronic records would be targeted by cybercriminals.

56. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

57. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Nelnet failed to take appropriate steps to protect Plaintiff and Class Members' PII from being compromised.

At All Relevant Times Nelnet Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

58. At all relevant times, Nelnet had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Nelnet became aware that their PII may have been compromised.

59. Nelnet's duty to use reasonable security measures arose as a result of the special relationship that existed between Nelnet, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted Nelnet and/or its affiliates with their PII when they were student loan borrowers.

60. Nelnet had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information.

Accordingly, Nelnet breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

61. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[17] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[17] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[18]

63. The ramifications of Nelnet's failure to keep its Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly financial information, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personal Identifiable Information

64. PII of data breach victims, like Plaintiff and Class Members, remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[20]

65. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[21]

---

[18] *Id.*

[19] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much- it-costs/ (last accessed December 10, 2021).

[20] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).

[21] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack- personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed

66. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[22]

67. Given the nature of Nelnet's Data Breach, as well as the delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII may easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

68. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, basic credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[23] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as dates of birth).

69. To date, Nelnet has only offered its Class Members twenty-four months of credit monitoring services even with the month delay from their discovery of the Data Breach to the production of the notice letters. The advice offered to victims in the notice letters is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

December 10, 2021).

[22] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[23] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1(last accessed December 10, 2021).

70. Plaintiff's and Class Members' injuries were directly and proximately caused by Nelnet's failure to implement or maintain adequate data security measures for the Class Members.

Nelnet Failed to Comply with FTC Guidelines

71. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[25] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

73. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[26]

74. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

---

[24] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed August 29, 2022).

[25] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed December 10, 2021).

[26] FTC, *Start with Security*, supra note 34.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

75. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. Because Class Members entrusted Nelnet with their PII directly or indirectly through Nelnet, Nelnet had, and has, a duty to the Class Members to keep their PII secure.

77. Plaintiff and the other Class Members reasonably expected that when they provide PII to Nelnet and/or its affiliates, that Nelnet would safeguard their PII.

78. Nelnet was at all times fully aware of its obligation to protect the personal data of borrowers, including Plaintiff and members of the Classes. Nelnet was also aware of the significant repercussions if it failed to do so.

79. Nelnet's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

80. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant and/or it affiliates with sensitive personal information, including their Social Security numbers.

81. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services, Plaintiff and other reasonable Class Members understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

82. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will

continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

83. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, contact information, financial information, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. stealing Social Security and other government benefits; and

f. applying for a driver's license, birth certificate, or other public document.

84. In addition, if a Class Member's Private Information is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

85. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

86. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[27]

[27] *Id.*

87. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[28] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[29] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[30] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

88. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

89. In its notice letter, Defendant represented to the Class Members and AGs that it initially discovered the Data Breach in July 2022, and admitted certain student loan registration information was accessed and acquired by the cybercriminals. As EmiSoft, an award-winning malware-protection software company, states "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, *especially during the preliminary stages of the investigation*."[31] It is likely that the cybercriminals did steal data and did so undetected.

---

[28] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed December 10, 2021).

[29] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed December 10, 2021).

[30] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA REACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS,(*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed December 10, 2021).

[31] EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than*

90. In this case, according to Defendant's notification to the Maine Attorney General, cybercriminals had access to Class Members' data from June 1, 2022, yet its notice letters about that Data Breach did not go out until August 26, 2022.[32] This is tantamount to the cybercriminals having nearly a three-month head start on stealing the identities of Plaintiff and Class Members.

91. Accordingly, that Defendant has not found evidence of data being misused is not an assurance that the data were not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

Plaintiff Varlotta's Experience

92. Plaintiff provided his personal information to Nelnet in conjunction with servicing related to Plaintiff's student loans.

93. As part of his involvement with Defendant, Plaintiff entrusted his PII, and other confidential information such as name, address, Social Security number, phone number, financial account information, and other personally identifiable information with the reasonable expectation and understanding that Nelnet would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify him of any data security incidents related to him. Plaintiff would not have permitted his PII to be given to Nelnet had he known it would not take reasonable steps to safeguard his PII.

94. On or about August 26, 2022, nearly three months after Nelnet's breach began, Plaintiff received a letter from Nelnet notifying him that his PII had been improperly accessed

---

one in ten (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen- in-a-ransomware-attack-is-greater-than-one-in-ten/ (last accessed December 13, 2021, emphasis added)).

[32] https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0.shtml

and taken by unauthorized third parties. The notice indicated that Plaintiff's PII was compromised as a result of the Data Breach.

95. As a result of the Data Breach, Plaintiff has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

96. Plaintiff spent this time at Defendant's direction. Indeed, in the Notice letter Plaintiff received, Defendant directed Plaintiff to take steps to mitigate his losses:

> We encourage you to remain vigilant against incidents of identity theft and fraud over the next 24 months, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Personal Information.*"

97. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Nelnet obtained from Plaintiff; (b) violation of his privacy rights; (c) the theft of his PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

98. As a result of the Data Breach, Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

99. The Data Breach has caused Plaintiff to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Social Security number and other intimate details are in the hands of criminals.

100. As a result of the Data Breach, Plaintiff anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

101. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

102. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated.

103. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons residing in the United States whose PII was compromised in the 2022 data breach announced by Nelnet Servicing, LLC in August 2022. (the "Nationwide Class").**

104. Excluded from the Classes are the following individuals and/or entities: Nelnet Servicing, LLC, and Nelnet's parents, subsidiaries, affiliates, officers and directors, and any entity in which Nelnet has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

105. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

106. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are 2,501,324 individuals

whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

107. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' PII;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' PII to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiff's and Class Members' PII for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

108. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

109. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

110. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

111. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

112. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

113. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

114. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

115. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach,

and Defendant may continue to act unlawfully as set forth in this Complaint.

116. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

117. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether a contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

e. Whether Defendant breached the contract;

f. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

g. Whether Defendant breached the implied contract;

h. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

118. Plaintiff restates and reallege all of the foregoing paragraphs as if fully set forth herein.

119. As a condition of having their student loans processed, Plaintiff and Class Members, as current and former student loan borrowers, are obligated to provide Nelnet and/or its affiliates with certain PII, including but not limited to, their name, date of birth, address, Social Security number, state-issued identification numbers, tax identification numbers, military identification numbers, and financial account numbers.

120. Plaintiff and Class Members entrusted their PII to Nelnet and its affiliates on the premise and with the understanding that Nelnet would safeguard their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

121. Nelnet has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

122. Nelnet knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and/or using of the PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

123. Nelnet had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Nelnet's security protocols to ensure that Plaintiff's and Class Members' information in Nelnet's possession was adequately secured and protected.

124. Nelnet also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

125. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Nelnet's business as sophisticated student loan service provider, for which the diligent protection of PII is a continuous forefront issue.

126. Plaintiff and Class Members were the foreseeable and probable victims of Nelnet's inadequate security practices and procedures. Nelnet knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Nelnet's systems.

127. Nelnet's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Nelnet's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Nelnet's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Nelnet.

128. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Nelnet's possession.

129. Nelnet was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

130. Nelnet had and continues to have a duty to adequately and promptly disclose that Plaintiff's and Class Members' PII within Nelnet's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair

any identity theft and the fraudulent use of their PII by third parties.

131. Nelnet had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII.

132. Nelnet has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

133. Nelnet, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII during the time the PII was within Nelnet's possession or control.

134. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

135. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

136. Nelnet improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

137. Nelnet failed to heed industry warnings and alerts to provide adequate safeguards to protect borrower PII in the face of increased risk of theft.

138. Nelnet, through its actions and/or omissions, unlawfully breached its duty to

Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

139. Nelnet, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

140. But for Nelnet's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

141. There is a close causal connection between Nelnet's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm suffered or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Nelnet's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

142. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Nelnet, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Nelnet's duty in this regard.

143. Nelnet violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Nelnet's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

144. Nelnet's violation of Section 5 of the FTC Act constitutes negligence *per se*.

145. Plaintiff and Class members are within the class of persons that the FTC Act was

intended to protect.

146. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class.

147. As a direct and proximate result of Nelnet's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Nelnet's goods and services they received.

148. As a direct and proximate result of Nelnet's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-

economic losses.

149. Additionally, as a direct and proximate result of Nelnet's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

150. Plaintiff re-alleges and incorporate by reference paragraphs above as if fully set forth herein.

151. Plaintiff and Class Members conferred a monetary benefit on Defendant and its affiliate student loan companies in the form of monetary payments—directly or indirectly—for providing student loan services to current and former borrowers.

152. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiff and Class Members.

153. The money that borrowers paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

154. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

155. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on

data security measures to secure Plaintiff's PII.

156. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII and that the borrowers paid for.

157. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

COUNT III
Breach of Express Contract
(On Behalf of Plaintiff and the Nationwide Class)

158. Plaintiff re-alleges and incorporates by reference the above paragraphs as if fully set forth herein.

159. This count is plead in the alternative to Count II (Unjust Enrichment) above.

160. Plaintiff and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current customers, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

161. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (all customers entering into the contracts), as Defendant's service was for student loan services for Plaintiff and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these services.

162. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

163. Defendant materially breached its contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

164. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

165. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

166. Plaintiff and Class Members are entitled to compensator, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

167. Plaintiff re-alleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

168. This count is plead in the alternative to Count II (Unjust Enrichment) above.

169. Plaintiff's and Class Members' PII was provided to Defendant as part of student loan services that Defendant provided to Plaintiff and Class Members.

170. Plaintiff and Class Members agreed to pay Defendant for its services.

171. Defendant and the Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning

the security of Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

172. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

173. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

174. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

175. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach.

176. Defendant further breached the implied contract by providing untimely notification to Plaintiff and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

177. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

178. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

179. Had Defendant disclosed that its data security was inadequate, neither the Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

180. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

181. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

182. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

183. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

184. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access and publication of their PII to criminal actors, as occurred with the Data Breach. The PII of Plaintiff and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

185. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

186. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party.

187. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

188. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

189. Plaintiff and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's, and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

190. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

191. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' intimate and sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

192. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

193. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Nelnet Servicing, LLC and that the Court grant the following:

A. For an Order certifying the Nationwide Classes and appointing Plaintiff and his Counsel to represent the certified Nationwide Class;

B. For equitable relief enjoining Nelnet from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:

i. prohibiting Nelnet from engaging in the wrongful and unlawful acts described herein;

ii. requiring Nelnet to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Nelnet to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Nelnet can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Nelnet to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Nelnet from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Nelnet to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Nelnet's systems on a periodic basis, and ordering Nelnet to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Nelnet to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Nelnet to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Nelnet to segment data by, among other things, creating firewalls and access controls so that if one area of Nelnet's network is compromised, hackers cannot gain access to other portions of Nelnet's systems;

x. requiring Nelnet to conduct regular database scanning and securing checks;

xi. requiring Nelnet to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Nelnet to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Nelnet to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Nelnet's

policies, programs, and systems for protecting personal identifying information;

xiv. requiring Nelnet to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Nelnet's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Nelnet to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Nelnet to implement logging and monitoring programs sufficient to track traffic to and from Nelnet's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Nelnet's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: September 2, 2022

Respectfully Submitted:

J.L. Spray, #18405
Jacob C. Garbison, #26789
MATTSON RICKETTS LAW FIRM
134 South 13th Street, Suite 1200
Lincoln, NE 68508
Telephone No.: (402) 475-8433
Fax No.: (402) 625-0775
Email: jls@mattsonricketts.com
jcg@mattsonricketts.com

COUNSEL FOR THE PLAINTIFF AND THE PUTATIVE CLASS

*Brandon M. Wise – IL Bar # 6319580
PEIFFER WOLF CARR KANE CONWAY & WISE, LLP
818 Lafayette Ave., Floor 2
St. Louis, MO 63104
Ph: 314-833-4825
Email: bwise@peifferwolf.com

**Application for admission submitted*

COUNSEL FOR THE PLAINTIFF AND THE PUTATIVE CLASS